Integrality and rigidity for postcritically finite polynomials

Adam Lawrence Epstein

October 15, 2010

1 Overview

Parameter spaces of algebraic dynamical systems are stratified according to various natural conditions, such as critical orbit relations, which may be imposed or broken. We consider monic polynomials of degree $d \geq 2$, over fields $\mathbb{K}$ of characteristic zero. Such a polynomial F is determined by a list of critical points $\mathbf{a} = (a_1, \ldots, a_{d-1})$ and the image $b = F(\bar{\mathbf{a}})$ of their barycenter

$$\bar{\mathbf{a}} = \frac{1}{d-1} \sum_{i=1}^{d-1} a_i.$$

This prescription yields a family $F_{\bar{\mathbf{a}},b}$ parametrized by $\mathbb{K}^{d-1} \times \mathbb{K}$.

The iterates of F are defined inductively as

$$F^0(z) = z \quad \text{and} \quad F^{n+1}(z) = F(F^n(z)).$$

The *forward orbit* of $\zeta \in \mathbb{K}$ is the sequence $F^n(\zeta)$, which is finite if and only if ζ is preperiodic. More generally, if $\mathbb{K}$ is equipped with a valuation ν, we say that ζ has *bounded* forward orbit if the sequence $\nu(F^n(\zeta))$ is bounded from below. We say F is *postcritically finite* (respectively, *postcritically bounded*) if the forward orbit of every critical point is finite (respectively, bounded).

An element ζ of a valued field $\mathbb{K}$ is *ν-integral* if $\nu(\zeta) \geq 0$; a ν-integral vector is one whose components are all ν-integral. For prime p, we denote by ν_p the p-adic valuation on $\mathbb{Q}$: that is, $\nu_p\left(p^e \cdot \frac{x}{y}\right) = e$ if neither integer x, y is a multiple of p. An algebraic number is ν-integral for one valuation

ν extending ν_p if and only if it is for any other, namely if it is the root of a monic polynomial whose coefficients are ν_p-integral rational numbers; thus, we may refer to such an algebraic number is p-integral.

Theorem 1 *Let $\mathbb{K}$ be a field extending $\mathbb{Q}$, equipped with a valuation ν extending ν_p. Assume that the degree of $F_{\mathbf{a},b}$ is a power of p, and suppose that $\bar{\mathbf{a}}$ is ν-integral. Then $F_{\mathbf{a},b}$ is postcritically bounded if and only if $\mathbf{a}$ and b are ν-integral.*

The result applies in particular to postcritically finite polynomials, and in this setting sharper results are sometimes possible, at least for certain families. Our interest here is the application of Theorem 1 to questions of rigidity. It is appropriate to work in the moduli space of translation conjugacy classes, or more concretely, the subspace $\bar{\mathbf{a}} = 0$ corresponding to *centered* polynomials. Given $(d-1)$-tuples of integers $\mathbf{m} = (m_1, \ldots, m_{d-1})$ and $\mathbf{n} = (n_1, \ldots, n_{d-1})$ with $0 \leq m_i < n_i$, consider the vanishing loci

$$V_i^{\mathbf{m},\mathbf{n}} = \mathbb{V}\left(\bar{\mathbf{a}}, F_{\mathbf{a},b}^{m_i}(a_i) - F_{\mathbf{a},b}^{n_i}(a_i)\right)$$

and their intersection $V^{\mathbf{m},\mathbf{n}} = \bigcap_{i=1}^{d-1} V_i^{\mathbf{m},\mathbf{n}}$.

Corollary 1 *Assume that d is a prime power. Then $V^{\mathbf{m},\mathbf{n}}$ is finite.*

Proof: Over an algebraically closed field, an algebraic set which is bounded relative to a nontrivial absolute value is necessarily zero-dimensional, hence finite, since any curve projects to a Zariski dense subset of some coordinate axis. In view of Theorem 1, the $\overline{\mathbb{Q}}$-points of $V^{\mathbf{m},\mathbf{n}}$ are p-integral, whence uniformly bounded relative to any p-adic absolute value. Consequently, there are only finitely many $\overline{\mathbb{Q}}$-points, and furthermore, by the Nullstellensatz, every point is a $\overline{\mathbb{Q}}$-point. $\square$

In the special case of periodic critical points, we have the following refinement:

Corollary 2 *Assume that d is a prime power. Then $V^{\mathbf{0},\mathbf{n}}$ consists entirely of simple points: near any point of their common intersection, the loci $V_i^{\mathbf{0},\mathbf{n}}$ are smooth, reduced hypersurfaces which are pairwise transverse.*

The proof of Corollary 2 is rooted in the well-known computation, usually attributed to Gleason, for monic centered quadratic polynomials: see the Appendix. Bobenrieth has carried out an analogous computation in the family $z \mapsto 1 + \frac{1}{wz^d}$ [1]. The case of cubic polynomials has also been treated by

Silverman, but with 3-integrality obtained differently, through explicit computation of resultants [10].

The restriction to prime power degree is not entirely an artifact of our arithmetic inexpertise. For $n \geq 2$, consider $\psi_n = s_n \circ g_n$, where $s_n(z) = z^n$ and $g_n(z) = \frac{(n+1)z - z^{n+1}}{n}$ (see [3, Section 4]). Note that g_n has fixed critical points, at the n-th roots of unity, so ψ_n has fixed critical values, at 0 and 1. Consequently, any composition $\psi_{n_\ell} \circ \cdots \circ \psi_{n_1}$ is postcritically finite. The leading coefficient of such a composition Ψ is of the form N^{-1} for an integer $N \neq \pm 1$. Conjugation by an appropriate homothety yields a monic centered postcritically finite polynomial having a critical point at a given root $N^{-1/(D-1)}$, where D is the degree of Ψ, and such a point cannot be ν_p-integral for any p dividing N. For example, ψ_2 rescales to $z^6 - (2^{1/5}3)z^4 + (2^{-8/5}3^2)z^2$ with a critical point at $2^{-2/5}$: this critical point is not 2-integral, and yet 2 divides the degree 6. In this case there is another prime dividing 6, namely 3, and all of the critical points are 3-integral. However, for the degree 72 polynomial $\psi_2 \circ \psi_3$ (respectively $\psi_3 \circ \psi_2$), the critical point $2^{-2/71}3^{-18/71}$ (respectively $-2^{-24/71}3^{-3/71}$) is not p-integral for either of the primes $p = 2, 3$ dividing 72. The appropriate extension of Theorem 1 remains a mystery.

On the other hand, Corollary 1 (without degree restrictions) is well-known through the use of complex analytic methods, as the analogous corollary of the boundedness of the *connectedness locus*: the set of parameters corresponding to polynomials which are postcritically bounded relative to the usual archimedean absolute value, or more customarily, whose Julia set over $\mathbb{C}$ is connected. Theorem 1 is a nonarchimedean version of this well-known boundedness principle, and our proof is similar in spirit. We imagine that the corresponding archimedean computation is folklore: the now classical argument in [2] relies on basic estimates from univalent function theory.

Corollary 2 (without degree restrictions) is also understood complex analytically, but the explanation is conceptually deeper. The relevant transversality is deduced in various ways. For example, [9] classifies the biholomorphism types of hyperbolic components, and verifies transversality by inspection of the models. The discussion in [4] from first principles of Teichmüller theory additionally yields appropriate transversality assertions in connection with preperiodic critical points. Both treatments are conceptually related to a fundamental rigidity principle due to Thurston (see [6] for discussion and proof of the Existence and Uniqueness Theorems). We remark that the algebraic content of Thurston Rigidity for polynomials is expressed by (un-

restricted) Corollary 1, and that the proof of Thurston Rigidity rests on an infinitesimal rigidity principle whose algebraic content, for polynomials with periodic critical points, is expressed by (unrestricted) Corollary 2.

Acknowledgments

We thank Bjorn Poonen and Joe Silverman for enlightening discussions of related matters. We thank Xander Faber for organizing the May, 2010 workshop on Moduli Spaces and the Arithmetic of Dynamical Systems, at the Bellairs Research Institute in Barbados, where these discussions arose. We thank Xavier Buff for suggesting [3, Section 4] as a source of counterexamples.

2 Integrality

Consider the polynomials

$$F_{\mathbf{a},b}(z) = z^d + \sum_{k=1}^{d-1}(-1)^{d-k}\frac{d}{k}\sigma_{d-k}z^k + b - \bar{\mathbf{a}}^d - \sum_{k=1}^{d-1}(-1)^{d-k}\frac{d}{k}\sigma_{d-k}\bar{\mathbf{a}}^k$$

where

$$\sigma_k = \sum_{1\le i_1<\cdots<i_k\le d-1}\prod_{j=1}^{k} a_{i_j}$$

are the elementary symmetric functions. Observe that b is the image of the barycenter $\bar{\mathbf{a}} = \frac{1}{d-1}\sum_{i=1}^{d-1} a_i$ of the (labeled) critical points $a_1, \ldots, a_{d-1}$. We denote by c the barycenter

$$\frac{1}{d-1}\sum_{i=1}^{d-1} F_{\mathbf{a},b}(a_i)$$

of the critical values. We set $\mathbf{a}^* = (a_1^*, \ldots, a_{d-1}^*)$, where $a_i^* = a_i - \bar{\mathbf{a}}$, and $b^* = b - \bar{\mathbf{a}}$, so that $F_{\mathbf{a},b}(z+\bar{\mathbf{a}}) = F_{\mathbf{a}^*,b^*}(z) + \bar{\mathbf{a}}$. Note that $c = b + \Phi(\mathbf{a}^*)$ where

$$\Phi(\mathbf{a}) = \frac{1}{d-1}\sum_{i=1}^{d-1}\left(a_i^d + \sum_{k=1}^{d-1}(-1)^{d-k}\frac{d}{k}\sigma_{d-k}a_i^k\right) - \bar{\mathbf{a}}^d - \sum_{k=1}^{d-1}(-1)^{d-k}\frac{d}{k}\sigma_{d-k}\bar{\mathbf{a}}^k$$

is homogeneous of degree d, and translation invariant: $\Phi(\mathbf{a}) = \Phi(\mathbf{a}^*)$.

The fact that the coefficients of $F_{\mathbf{a},b}$ lie in $\mathbb{Q}$, but not necessarily in $\mathbb{Z}$, is a source of complication. However, under favorable conditions, these coefficients do belong to appropriate local rings $\mathbb{Z}_{(p)}$.

Lemma 1 *Assume that d is a power of a prime p. Then:*

- $F_{\mathbf{a},b}(z) \equiv z^d + b - \bar{\mathbf{a}}^d \pmod{p}$ *in* $\mathbb{Z}_{(p)}[a_1 \ldots, a_{d-1}, b][z]$,
- $\Phi(\mathbf{a}) \equiv 0 \pmod{p}$ *in* $\mathbb{Z}_{(p)}[a_1, \ldots a_{d-1}]$.

Proof: Note that if $p|d$ then $\frac{1}{d-1} \in \mathbb{Z}_{(p)}$ so $\bar{\mathbf{a}} \in \mathbb{Z}[a_1, \ldots, a_{d-1}]$. Moreover, if d is a power of p then $\nu_p\left(\frac{d}{k}\right) \geq 1$ for $1 \leq k \leq d-1$, and furthermore

$$\Phi(\mathbf{a}) \equiv \frac{1}{d-1}\sum_{i=1}^{d-1} a_i^d - \left(\frac{1}{d-1}\sum_{i=1}^{d-1} a_i\right)^d \pmod{p}.$$

Now

$$\left(\sum_{i=1}^{d-1} a_i\right)^d = \sum_{(m_1 \ldots m_{d-1})} \binom{d}{m_1 \ldots m_{d-1}} \prod_{i=1}^{d-1} a_i^{m_i}$$

summed over $(d-1)$-tuples of integers $m_i \geq 0$ with $\sum\limits_{i=1}^{d-1} m_i = d$. Since

$$\nu_p(n!) = \sum_{e=1}^{\infty} \left\lfloor \frac{n}{p^e} \right\rfloor$$

for any n, we have

$$\nu_p\left(\binom{n}{m_1 \ldots m_{d-1}}\right) = \nu_p(n!) - \sum_{i=1}^{d-1} \nu_p(m_i!) = \sum_{e=1}^{\infty}\left(\left\lfloor \frac{n}{p^e} \right\rfloor - \sum_{i=1}^{d-1} \left\lfloor \frac{m_i}{p^e} \right\rfloor\right)$$

where $\left\lfloor \frac{n}{p^e} \right\rfloor \geq \sum\limits_{i=1}^{d-1} \left\lfloor \frac{m_i}{p^e} \right\rfloor$ for every $e \geq 1$. Thus, if $d = p^e$ and all $m_i < d$ then

$$\nu_p\left(\binom{d}{m_1 \ldots m_{d-1}}\right) \geq \left\lfloor \frac{p^e}{p^e} \right\rfloor - \sum_{i=1}^{d-1} \left\lfloor \frac{m_i}{p^e} \right\rfloor = 1,$$

hence $\left(\sum\limits_{i=1}^{d-1} a_i\right)^d \equiv \sum\limits_{i=1}^{d-1} a_i^d \pmod{p}$. Since $d|((d-1)^{d-1} - 1)$, it follows that

$$\Phi(\mathbf{a}) \equiv ((d-1)^{d-1} - 1)\bar{\mathbf{a}}^d \equiv 0 \pmod{p}.$$

□

Let ν be a valuation extending ν_p, where $p|d$. For $(\mathbf{a}, b) \in \mathbb{K}^{d-1} \times \mathbb{K}$, set

$$\mu_{\mathbf{a},b} = \inf \left\{ \nu(\zeta - \bar{\mathbf{a}}) : \text{ the forward orbit } F^n_{\mathbf{a},b}(\zeta) \text{ is bounded} \right\}.$$

Since $\nu(F^n_{\mathbf{a},b}(\zeta) - F^n_{\mathbf{a}^*,b^*}(\zeta^*)) = \nu(\bar{\mathbf{a}})$ is constant, for any $\zeta \in \mathbb{K}$ and $\zeta^* = \zeta - \bar{\mathbf{a}}$, the forward orbit $F^n_{\mathbf{a},b}(\zeta)$ is bounded if and only if the forward orbit $F^n_{\mathbf{a}^*,b^*}(\zeta^*)$ is bounded. It follows that $\mu_{\mathbf{a},b} = \mu_{\mathbf{a}^*,b^*}$ and that $F_{\mathbf{a},b}$ is postcritically bounded if and only if $F_{\mathbf{a}^*,b^*}$ is postcritically bounded.

Lemma 2 *For any $(\mathbf{a}, b) \in \mathbb{K}^{d-1} \times \mathbb{K}$, we have*

$$\mu_{\mathbf{a},b} \geq \min\left(\alpha + \epsilon, \frac{\beta}{d}, 0\right)$$

where $\alpha = \min\limits_{1 \leq i \leq d-1} \nu(a_i - \bar{\mathbf{a}})$ and $\beta = \nu(b - \bar{\mathbf{a}})$, and $\epsilon = \min\limits_{1 \leq k \leq d-1} \frac{\nu\left(\frac{d}{k}\right)}{d-k}$.

Proof: Since the statement is translation invariant, we may assume without loss of generality that $\bar{\mathbf{a}} = 0$, so $\alpha = \min\limits_{1 \leq i \leq d-1} \nu(a_i)$ and therefore

$$\nu\left(\frac{d}{k}\right) + (d-k)\alpha + \nu(\zeta^k) \leq \nu\left(\frac{d}{k}\sigma_{d-k}\zeta^k\right).$$

Thus, if $\nu(\zeta) < \alpha + \frac{\nu\left(\frac{d}{k}\right)}{d-k}$ then $\nu(\zeta^d) = \nu(\zeta^{d-k}) + \nu(\zeta^k) < \nu\left(\frac{d}{k}\sigma_{d-k}\zeta^k\right)$, so if $\nu(\zeta) < \alpha + \epsilon$ then $\nu(\zeta^d) < \nu\left(\frac{d}{k}\sigma_{d-k}\zeta^k\right)$ for $1 \leq k \leq d-1$, whence if $\nu(\zeta) < \min\left(\alpha + \epsilon, \frac{\beta}{d}\right)$ then $\nu(F_{\mathbf{a},b}(\zeta)) = \nu(\zeta^d) = d\nu(\zeta)$. Consequently, if $\nu(\zeta) < \min\left(\alpha + \epsilon, \frac{\beta}{d}, 0\right)$ then $\nu(F_{\mathbf{a},b}(\zeta)) = d\nu(\zeta) < \nu(\zeta) < \min\left(\alpha + \epsilon, \frac{\beta}{d}, 0\right)$, whence $\nu(F^n_{\mathbf{a},b}(\zeta)) = d^n\nu(\zeta) \to -\infty$. $\square$

Proof of Theorem 1: As above, we may assume without loss of generality that $\bar{\mathbf{a}} = 0$. By Lemma 1, since d is a power of p we have $\epsilon = \frac{1}{d-1} > 0$ and moreover $\nu(c - b) = \nu(\Phi(\mathbf{a})) \geq 1 + d\alpha$, since Φ is homogeneous of degree d. Now if $F_{\mathbf{a},b}$ is postcritically bounded then $\alpha \geq \mu_{\mathbf{a},b}$, hence $\mu_{\mathbf{a},b} \geq \min\left(\frac{\beta}{d}, 0\right)$, and $\nu(c) \geq \min\limits_{1 \leq k \leq d-1} \nu(F_{\mathbf{a},b}(a_i)) \geq \mu_{\mathbf{a},b}$. Thus,

$$\beta \geq \min(\nu(c), \nu(c-b)) \geq \min(\mu_{\mathbf{a},b}, 1 + d\mu_{\mathbf{a},b}) \geq \min\left(\frac{\beta}{d}, 0, 1 + \beta, 1\right)$$

so $\beta \geq \min\left(\frac{\beta}{d}, 0\right)$, hence $\beta \geq 0$, whence $\alpha \geq \mu_{\mathbf{a},b} \geq \frac{\beta}{d} \geq 0$: that is, $\mathbf{a}$ and b are ν-integral. Conversely, if $\mathbf{a}$ and b are ν-integral then since $\epsilon \geq 0$ the

coefficients of $F_{\mathbf{a},b}$ are ν-integral, so the postcritical points are ν-integral, whence $F_{\mathbf{a},b}$ is postcritically bounded. $\square$

The well-known considerations of Lemma 2 establish the existence and basic properties of the *local canonical height* functions

$$h_{\mathbf{a},b}(\zeta) = \lim_{n\to\infty} \frac{1}{d^n} \max(-\nu(F^n_{\mathbf{a},b}(\zeta), 0))$$

as discussed in the arithmetic dynamics literature [11]; in these terms, $F_{\mathbf{a},b}$ is postcritically bounded if and only if $H_{\mathbf{a},b} = 0$, where

$$H_{\mathbf{a},b} = \max_{1\le i\le d-1} h_{\mathbf{a},b}(a_i).$$

These quantities are evidently the nonarchimedean analogues of the Green's functions used in the classical proof of the boundedness of the connected locus in the archimedean case.

3 Simplicity

Recall that the loci $V^{\mathbf{m},\mathbf{n}}$ were defined in terms of the parameter subspace of centered polynomials $F_{\mathbf{a},b}$. Here it will be convenient to work with the variant family

$$\mathcal{F}_{\mathbf{a}}(z) = z^d + \sum_{k=1}^{d-1} (-1)^{d-k} \frac{d}{k} \sigma_{d-k} z^k$$

normalized to fix 0. Since d is a power of p, it follows from Lemma 1 that $\mathcal{F}_{\mathbf{a}}(z) \equiv z^d \pmod p$ in $\mathbb{Z}_{(p)}[a_1, \dots, a_{d-1}, b][z]$. Consequently,

$$\frac{\partial \mathcal{F}_{\mathbf{a}}(w)}{\partial a_i} = dw^{d-1} \frac{\partial w}{\partial a_i} \equiv 0 \pmod p$$

for $1 \le i \le d-1$ and any $w \in \mathbb{Z}_{(p)}[a_1, \dots, a_{d-1}, b]$.

Note that translation by $\bar{\mathbf{a}}$ conjugates $\mathcal{F}_{\mathbf{a}}$ to $F_{\mathbf{a}^*,b^*}$ where

$$(\mathbf{a}^*, b^*) = (a_1 - \bar{\mathbf{a}}, \dots, a_{d-1} - \bar{\mathbf{a}}, \mathcal{F}_{\mathbf{a}}(\bar{\mathbf{a}}) - \bar{\mathbf{a}}).$$

Conversely, if $\bar{\mathbf{a}}^\star = 0$ then any fixed point ξ of $F_{\mathbf{a}^\star,b^\star}$ we have $(\mathbf{a}^\xi)^* = \mathbf{a}^\star$ for $\mathbf{a}^\xi = (a_1^\star - \xi, \dots, a_{d-1}^\star - \xi)$. Observe that the map $\mathbf{a} \mapsto (\mathbf{a}^*, b^*) = \Lambda(\mathbf{a})$ sends each locus $\mathcal{V}_i^{\mathbf{m},\mathbf{n}} = \mathbb{V}(\mathcal{F}_{\mathbf{a}}(a_i) - a_i)$ onto the corresponding locus $V_i^{\mathbf{m},\mathbf{n}}$.

Moreover, Λ respects p-integrality: if $\mathbf{a}$ is p-integral then $\bar{\mathbf{a}}$ is p-integral, hence $(\mathbf{a}^*, b^*)$ is also p-integral, while if $(\mathbf{a}^\star, b^\star)$ is p-integral then, by monicity, any fixed point ξ of $F_{\mathbf{a}^\star, b^\star}$ is p-integral, whence $\mathbf{a}^\xi$ is p-integral.

Proof of Corollary 2: We claim that Λ is nonsingular at every p-integral $\mathbf{a}$. Indeed, the derivative of the composition $\mathbf{a} \mapsto (\mathbf{a}^*, b^*) \mapsto (a_1, \ldots, a_{d-2}, b)$ is given by the $(d-1) \times (d-1)$ matrix

$$\begin{pmatrix} 1 - \frac{1}{d-1} & -\frac{1}{d-1} & \cdots & -\frac{1}{d-1} & -\frac{1}{d-1} \\ -\frac{1}{d-1} & 1 - \frac{1}{d-1} & \cdots & -\frac{1}{d-1} & -\frac{1}{d-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ -\frac{1}{d-1} & -\frac{1}{d-1} & \cdots & 1 - \frac{1}{d-1} & -\frac{1}{d-1} \\ \frac{\partial \mathcal{F}_{\mathbf{a}}(\bar{\mathbf{a}})}{\partial a_1} - \frac{1}{d-1} & \frac{\partial \mathcal{F}_{\mathbf{a}}(\bar{\mathbf{a}})}{\partial a_2} - \frac{1}{d-1} & \cdots & \frac{\partial \mathcal{F}_{\mathbf{a}}(\bar{\mathbf{a}})}{\partial a_{d-2}} - \frac{1}{d-1} & \frac{\partial \mathcal{F}_{\mathbf{a}}(\bar{\mathbf{a}})}{\partial a_{d-1}} - \frac{1}{d-1} \end{pmatrix},$$

and since $\bar{\mathbf{a}} \in \mathbb{Z}_{(p)}[a_1, \ldots, a_{d-1}, b]$, this matrix is congruent (mod p) to

$$\begin{pmatrix} 0 & -1 & \cdots & -1 & -1 \\ -1 & 0 & \cdots & -1 & -1 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ -1 & -1 & \cdots & 0 & -1 \\ -1 & -1 & \cdots & -1 & -1 \end{pmatrix}$$

which has determinant $-1 \not\equiv 0$. In view of Theorem 1, every point of $V^{\mathbf{0},\mathbf{n}}$ is p-integral. It follows from the remarks above that Λ yields local isomorphisms, respecting integrality, between neighborhoods of points in $\mathcal{V}^{\mathbf{0},\mathbf{n}}$ and neighborhoods of the corresponding points in $V^{\mathbf{0},\mathbf{n}}$. Moreover, proving simplicity for $\mathcal{V}^{\mathbf{0},\mathbf{n}}$ amounts to observing the invertibility of $\mathbf{I} - \mathbf{F}$, where $\mathbf{I}$ is the $(d-1) \times (d-1)$ identity matrix, and where

$$\mathbf{F} = \begin{pmatrix} \frac{\partial \mathcal{F}_{\mathbf{a}}^{n_1}(a_1)}{\partial a_1} & \cdots & \frac{\partial \mathcal{F}_{\mathbf{a}}^{n_1}(a_1)}{\partial a_{d-1}} \\ \cdots & \cdots & \cdots \\ \frac{\partial \mathcal{F}_{\mathbf{a}}^{n_{d-1}}(a_{d-1})}{\partial a_1} & \cdots & \frac{\partial \mathcal{F}_{\mathbf{a}}^{n_{d-1}}(a_{d-1})}{\partial a_{d-1}} \end{pmatrix} \equiv 0 \pmod{p}$$

since $\mathcal{F}_{\mathbf{a}}^{n_i - 1}(a_i) \in \mathbb{Z}_{(p)}[a_1, \ldots, a_{d-1}]$ for $1 \leq i \leq d-1$. $\square$

Appendix (joint with Bjorn Poonen)

Consider the family of monic centered unicritical polynomials $F_{\mathbf{0},b}(z) = z^d + b$, where d is any integer greater than 1. For $n \geq 0$, we set $\Gamma_n = F_{\mathbf{0},b}^n(0) \in \mathbb{Z}[b]$.

Note that $\Gamma_0 = 0$, and that Γ_n is monic of degree 2^{n-1}, for $n \geq 1$. Thus, for $N > n \geq 0$ the polynomials $\Gamma_N - \Gamma_n \in \mathbb{Z}[b]$ are monic, whence their zeros in $\overline{\mathbb{Q}}$ are algebraic integers, in accordance with Theorem 1.

Here we extend Corollary 2 to all postcritically finite parameters in these families. The case of periodic critical point is straightforward. For $p = d = 2$, the following observation, already contained in Corollary 2, is due to Andrew Gleason (see [5, Lemma 19.1]), and independently to Allen Adler:

Proposition 1 *For $N \geq 1$, all zeros of Γ_N are simple.*

Proof: By definition, $\Gamma_N = (\Gamma_{N-1})^d + b$, so $\Gamma'_N = d(\Gamma_{N-1})^{d-1}\Gamma'_{N-1} + 1$, and thus $\Gamma'_N \equiv 1 \pmod{p}$ for any prime $p|d$. It follows that $\Gamma'_N(b) \neq 0$ for every algebraic integer b, in particular, for every zero of Γ_N. $\square$

The case of strictly preperiodic critical point is more subtle. For $d = 2$ this is treated in [7, Lemma 1, page 333], but the proof is incomplete when $n = 2$, since the discussion presumes that $\Gamma'_{n-2} \equiv 1 \pmod{2}$.

Theorem 2 *For $N > n \geq 1$, every multiple zero of $\Gamma_N - \Gamma_n$ is a zero of $\Gamma_{N-1} - \Gamma_{n-1}$.*

Proof: Observe that $\Gamma_N - \Gamma_n = (\Gamma_{N-1})^d - (\Gamma_{n-1})^d = \prod_\omega \Delta^\omega_{N,n}$ where $\Delta^\omega_{N,n} = \Gamma_{N-1} - \omega\Gamma_{n-1}$ and where the product is over the d-th roots of unity. If $\omega_1 \neq \omega_2$ then any common zero of $\Delta^{\omega_1}_{N,n}$ and $\Delta^{\omega_2}_{N,n}$ is also a zero of Γ_{N-1} and Γ_{n-1}, whence a zero of $\Delta^\omega_{N,n}$ for every ω, in particular for $\omega = 1$. Thus, it suffices to show that if $\omega \neq 1$ then all zeros of $\Delta^\omega_{N,n}$ are simple. Since every zero of $\Gamma_N - \Gamma_1 = (\Gamma_{N-1} - \Gamma_0)^d$ is a zero of $\Gamma_{N-1} - \Gamma_0$, we may assume without loss of generality that $n \geq 2$, whence $\Gamma'_{N-1} \equiv 1 \equiv \Gamma_{n-1} \pmod{p}$ for any prime $p|d$. It follows that if ν is a valuation extending ν_p then $\nu(\Delta^{\omega\prime}_{N,n}(b) - (1-\omega)) \geq 1$ for every algebraic integer b; this holds in particular for the zeros of $\Delta^\omega_{N,n}$, so if $\nu(1-\omega) < 1$ then these zeros are simple.

Each ω is a primitive m-th root of unity for some $1 \neq m|d$. If $m = p^e$ for some $e \geq 1$ then $\nu(1-\omega) = (p-1)p^{e-1}$ for any ν extending ν_p, while if m is not a prime power then $1 - \omega$ is a unit so $\nu(1-\omega) = 0$ for any valuation ν: for details, see [8, page 73]. Since $(p-1)p^{e-1} > 1$ except when $p = 2$ and $e = 1$, it follows that if $m \neq 2$ then there exists $p|d$ such that $\nu(1-\omega) < 1$ for any ν extending ν_p. Furthermore, if $m = 2$ then $\omega = -1$, so if d has an odd prime factor p then $\nu(1-\omega) = \nu_p(2) = 0$. These considerations establish simplicity in all cases except when $\omega = -1$ and d is a power of 2.

Suppose finally that $\omega = -1$ and $d = 2^e$ for some $e \geq 1$. In this case, ${\Delta^\omega}'_{N,n} = {\Gamma'}_{N-1} + {\Gamma'}_{n-1} = d\Lambda + 2$ where $\Lambda = (\Gamma_{N-2})^{d-1}{\Gamma'}_{N-2} + (\Gamma_{n-2})^{d-1}{\Gamma'}_{n-2}$. Consequently, it suffices to show that $\Delta^\omega_{N,n}(b) = 0$ implies $\nu(\Lambda(b)) > 0$, since then $\nu(d\Lambda(b)) > e \geq 1 = \nu(2)$. Observe that if $\nu(x), \nu(y) \geq 0$ then $\nu((x+y)-(x-y)) = \nu(2y) \geq 1$, so if $\nu(x-y) = 0$ then $\nu(x+y) = 0$, hence $\nu(x^2 - y^2) = 0$, and thus $\nu(x^{2^k} - y^{2^k}) = 0$ for $k \geq 0$; in particular, since $F_{\mathbf{0},b}(x) - F_{\mathbf{0},b}(y) = x^{2^e} - y^{2^e}$, it follows that $\nu(F_{\mathbf{0},b}(x) - F_{\mathbf{0},b}(y)) > 0$ implies $\nu(x-y) > 0$. Now if $\Delta^\omega_{N,n}(b) = 0$ then $F^2_{\mathbf{0},b}(\Gamma_{N-2}(b)) = F^2_{\mathbf{0},b}(\Gamma_{n-2}(b))$, so $\nu(\Gamma_{N-1}(b) - \Gamma_{n-1}(b)) > 0$ and thus $\nu(\Gamma_{N-2}(b) - \Gamma_{n-2}(b)) > 0$. If $n > 2$ then $\nu({\Gamma'}_{N-2}(b) - 1), \nu({\Gamma'}_{n-2}(b) - 1) \geq 1$, and thus $\nu({\Gamma'}_{N-2}(b) + {\Gamma'}_{n-2}(b)) \geq 1$; since $\nu(\Gamma_{N-2}(b)^{d-1} - \Gamma_{n-2}(b)^{d-1}) > 0$ and $\nu(\Gamma_{n-2}(b)) \geq 0$, we have $\nu(\Lambda(b)) > 0$. If $n = 2$ then $\Gamma_{n-2}(b) = 0$ so $\nu(\Gamma_{N-2}(b)) > 0$; since $\nu({\Gamma'}_{N-2}(b)) \geq 0$, it follows that $\nu(\Lambda(b)) > 0$ in this case as well. $\square$

References

[1] J. Bobenrieth, The multiplier map on hyperbolic components of a family of rational maps, 2000 manuscript.

[2] B. Branner & J. H. Hubbard, The iteration of cubic polynomials. Part I: The global topology of parameter space, *Acta. Math.* **160** (1988), 143-206.

[3] X. Buff, A. Epstein, S. Koch & K. Pilgrim, On Thurston's pullback map, in *Complex dynamics, families and friends*, ed. D. Schleicher, A. K. Peters, 2009.

[4] A. Epstein, Transversality in holomorphic dynamics, 2010 manuscript, `http://www.warwick.ac.uk/~mases/Transversality.pdf`.

[5] A. Douady & J. H. Hubbard, Exploring the Mandelbrot set, *The Orsay notes*, `http://www.math.cornell.edu/~hubbard/OrsayEnglish.pdf`.

[6] A. Douady & J. H. Hubbard, A proof of Thurston's topological characterization of rational functions, *Acta Math.* **171** (1993), 263-297.

[7] A. Douady & J. H. Hubbard, On the dynamics of polynomial-like mappings, *Ann. Sci. Ec. Norm. Sup.* 4^e Ser. **18** (1985), 287-344.

[8] S. Lang, *Algebraic number theory*, Springer-Verlag, 1986.

[9] J. Milnor, Hyperbolic components in spaces of polynomial maps, `http://arxiv.org/abs/math/9202210`.

[10] J. Silverman, *An algebraic approach to Thurston rigidity*, 2010 manuscript.

[11] J. Silverman, *The arithmetic of dynamical systems*, Springer-Verlag, 2007.